



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/738,893

12/15/2000

Yannick Teglia

99-RO-182

2162

23334 7590 10/19/2006

FLEIT, KAIN, GIBBONS, GUTMAN, BONGINI
& BIANCO P.L.
ONE BOCA COMMERCE CENTER
551 NORTHWEST 77TH STREET, SUITE 111
BOCA RATON, FL 33487

EXAMINER

KHOSHNOODI, NADIA

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/738,893

Applicant(s)

TEGLIA, YANNICK

Examiner

Nadia Khoshnoodi

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9-14, 16, 17, 19-22 and 24-28 is/are pending in the application.
- 4a) Of the above claim(s) 8, 15, 18 and 23 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7, 9-14, 16, 17, 19-22 and 24-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/7/2006 has been entered.

Response to Amendment

Claims 8, 15, 18, & 23 have been cancelled. Applicant's arguments/amendments with respect to amended claims 1-2, 13-14, 16, 21-22, & 24; previously presented claims 3-7, 9-10, 17, 19-20; and newly presented claims 25-28 filed 8/7/2006 have been fully considered but are moot in view of new grounds rejection (with regards to the amended claims). However, various arguments with respect to the Pfab reference (which have been fully considered) are not persuasive.

Applicant contends that Pfab does not disclosed a method for secured transfer of the an N-byte data element in which the value of at least one parameter of a transfer rule defining the order in which the bytes of the data elements are transferred is randomly chosen before each transfer of the data element, and the N-byte data element is transferred byte-by-byte in the order specified by the transfer rule. Examiner respectfully disagrees with Applicant on these points. Pfab teaches the secure transfer of data bits, i.e. an N-byte data element (col. 2, lines 57-65). Furthermore, Pfab also teaches transfer rules (in the encoding process) by addressing that the

Art Unit: 2137

encoding module determines which bit lines should be used, as well as how the significance of different bits can be altered (col. 6, lines 44-57). Pfab's disclosure of altering the significance of different bits is equivalent to that of defining the order in which the bytes are transferred because of the fact that 1 byte consists of eight bits. Furthermore, Pfab's disclosure of determining which bit lines should be used also determines the byte order in which the N-byte data element will progress through the bus. Pfab also teaches that the key, i.e. a parameter of the transfer rule, can be randomly selected (col. 4, lines 52-57). Finally Pfab teaches that the data element is transferred byte-by-byte because a sequence of eight bits is equivalent to one byte and there is an operating module that can influence the encoding using different conversion methods (col. 5, lines 19-26).

Furthermore, Applicant contends that Pfab does not disclose a programmable circuit that includes a random number generator that supplies the value of at least one parameter of a data transfer rule that defines the order in which the bytes of the data element are transferred before each transfer of the data element and a control unit that controls a data bus that the N-byte data elements is transferred byte-by-byte in the order specified by the data transfer rule. Examiner respectfully disagrees with Applicant on these points for the reasons discussed above.

Furthermore, Pfab specifically teaches an electronic data processing circuit including a random number generator for randomly selecting a key, i.e. the parameter of the transfer rule (claim 14). Pfab also teaches a control unit that controls the data bus in order to send the data bits, where eight bits is equivalent to one byte and therefore the option of sending data elements byte-by-byte is available because it is commonly know in the art (col. 8, lines 15-62).

Art Unit: 2137

Finally, Applicant contends that Pfab does suggest using a permutation to encode the data, but does not teach or suggest using a permutation of the bytes of an N-byte data element such that each transfer of the N-byte data element is not done in the same byte order. Examiner agrees that Pfab suggests using a permutation to encode the data, but respectfully disagrees with Applicant that this does not imply a permutation of the bytes of an N-byte data element so that each transfer of the N-byte data element is not done in the same byte order. Data is broken up into bits, where eight bits is equivalent to one byte. Therefore, since a permutation is being used to encode the data bits, it ensures that there is also a permutation of the bytes of an N-byte data element based on the fact that a byte is broken up into eight bits. Hence, each transfer of the N-byte data element is not done in the same byte order (col. 3, lines 40-49 and col. 8, lines 15-62). Furthermore, since there are different data lines that can be used to transfer the data elements, the bytes are still not transferred in the same byte order (col. 8, lines 1-50).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned

Art Unit: 2137

with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

I. Claims 1, 14, and 22 are rejected on the ground of nonstatutory double patenting over claims 1 and 16 of U.S. Patent No. 7,116,783. Although the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter claimed in the instant application is fully disclosed in the referenced patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows:

Claims 1 & 14 of the present application and claim 1 of the referenced patent both claim steps for transferring an N-byte data element byte-by-byte from the first memory to the second memory according to a transfer rule (which is defined starting line 12 of claim 1 in the patent), where a parameter of the transfer rule is randomly selected (the "current index" in claim 1 of the patent) to result in a randomly selected order in which to send the bytes at least one time through the data bus. Thus, the limitations in claims 1 and 14 are fully anticipated by claim 1 from US Patent No. 7,116,783.

Claim 22 of the present application and claim 16 of the referenced patent both claim a data bus, a read-only memory containing an N-byte data element to be transferred where the ROM is coupled to the data bus, a writable memory coupled to the data bus, a control unit coupled to the ROM and writable memory, a random number generator coupled to the control unit where the random number generator supplies a parameter, with various other identical

Art Unit: 2137

components for transferring an N-byte data element byte-by-byte from the first memory to the second memory according to a transfer rule (which is defined starting line 19 of claim 16 in the patent), where a parameter of the transfer rule is randomly selected (the "current index" in claim 16 of the patent) to result in a randomly selected order in which to send the bytes at least one time through the data bus. Thus, the limitations in claim 22 are fully anticipated by claim 16 from US Patent No. 7,116,783.

Claim Rejections - 35 USC § 103

II. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

III. Claims 1-2, 14, 22, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Iida, US Patent No. 5,422,727, and further in view of Pfab, US Patent No. 6,195,752.

As per claims 1, 14, and 22:

Iida substantially teaches a method/machine-readable medium encoded with instructions/programmable circuit comprising: providing an N-byte data element in the first memory (col. 9, lines 12-23); and successively transferring the N-bytes of the data element byte-by-byte through the data bus to the second memory, with each of the N bytes transisting once and only once through the data bus (col. 9, lines 44-49).

Not explicitly disclosed is randomly choosing the value of at least one parameter of a transfer rule before a transfer of the N-byte data element, the transfer rule defining the order in which the bytes of the N-byte data element are successively transferred through the data bus. However, Pfab teaches a FLASH memory through a data line, connected to a multiplexer, which is connected to the ROM (col. 8, lines 50-57), multiplexer being fed a random number by a random number generator over a data line (col. 8, lines 51-57), and the encoding method having the ability to define interchanging individual bit lines of the data bus, or altering the significance of individual data bits as the transfer rule (col. 6, lines 54-56). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Iida for the parameter (key) to be randomly selected and used in the encoding/decoding method which takes place before the transferring of the N-byte data element from one memory to the next and which defines the order in which the data elements are transferred. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pfab suggests that using the previously mentioned method will result in substantially increasing security against manipulations in col. 5, lines 19-27 and lines 44-66.

As per claim 2:

Iida and Pfab substantially teach the method of claim 1. Furthermore, Pfab teaches wherein the encoding or decoding, occurring upon transferring the data, can be performed by a suitable delay, by interchanging individual bit lines of the data bus, or by altering the significance of individual data bits indicating that in each transfer of the N-byte data element the

Art Unit: 2137

N bytes do not successively transit through the data bus in the same byte order (col. 6, lines 53-57).

As per claim 25:

Iida and Pfab substantially teach the method of claim 1. Furthermore, Iida teaches wherein in the successively transferring step, each of the bytes of the data element is transferred through the data bus without changing the order of bits of that byte (col. 9, lines 44-49).

As per claim 26:

Iida and Pfab substantially teach the method of claim 1. Furthermore, Iida teaches wherein each byte of the data element has the same bit order in the first memory, while transiting through the data bus, and in the second memory (col. 9, lines 44-49).

As per claim 27:

Iida and Pfab substantially teach the method of claim 1. Furthermore, Pfab teaches that the successively transferring step includes the sub-step of: before each successive transfer of one of the bytes of the data element, using the transfer rule to determine a place value of the byte of the N-byte data element to be transferred (col. 6, lines 53-57), at each successive transfer of one of the bytes of the data element, transferring the byte of the N-byte data element with the place value that was determined by the transfer rule (col. 6, lines 57-65), repeating the using and transferring sub-steps N times so as to successively transfer the N bytes of the data element through the data bus (col. 5, lines 51-61).

As per claim 28:

Iida and Pfab substantially teach the method of claim 1. Furthermore, Pfab teaches that the successively transferring step includes the sub-step of: first transferring one byte of the N-

Art Unit: 2137

byte data element whose place value is defined by the transfer rule (col. 6, lines 53-57); after the first transferring sub-step, transferring another byte of the N-byte data element whose place value is defined by the transfer rule (col. 6, lines 57-65); repeating the sub-step of transferring another byte until the N bytes of the data element have been successively transferred through the data bus in the order specified by the transfer rule (col. 6, lines 53-65).

IV. Claims 3-7, 9-13, 16-17, 19-21, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Iida, US Patent No. 5,422,727, and Pfab, US Patent No. 6,195,752 and further in view of Menezes, *Handbook of Applied Cryptography*.

As per claim 3:

Iida and Pfab substantially teach the method of claim 2. Not explicitly disclosed is the permutation is defined by the relationship: $X = (XO + \text{DIRECTION} * \text{PITCH} * j) \text{ modulo } N$ where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, XO ranges from 0 to N-1, and j varies from 0 to N-1. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). A different permutation algorithm is commonly known in the art, it would have been obvious to one skilled in the art at the time of the invention was made to use a particular formula to permute a given incoming data. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including a permutation into the algorithm, $X = (XO + \text{DIRECTION} * \text{PITCH} * j) \text{ modulo } N$, using data transfer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements. The data elements are securely transferred in order to allow only authorized individuals to obtain the data.

Art Unit: 2137

As per claim 4:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is in the defining step, the value of PITCH is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 5:

Iida and Pfab substantially teach the method of claim 4. Not explicitly disclosed is in the defining step, the value of DIRECTION is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 6:

Art Unit: 2137

Iida and Pfab substantially teach the method of claim 5. Not explicitly disclosed is in the defining step, the value of XO is chosen randomly before each transfer of the data element.

Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 7:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is in the defining step, the value of PITCH is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 9:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is in the defining step, the value of XO is chosen randomly before each transfer of the data element.

Art Unit: 2137

Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 10:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is where in the defining step, the value of PITCH and the value of XO are chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 11:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is where PITCH and N are mutually prime numbers. Menezes teaches mutually prime numbers, relatively prime, or coprime if $\text{gcd}(a,b) = 1$ (pg. 64, section 2.91). Therefore, it would have been obvious to

Art Unit: 2137

a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including mutually prime numbers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to not have degenerate permutation functions, therefore enhancing the security of the data transfer.

As per claim 12:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is where N is a prime integer and $PITCH$ is an integer ranging from 1 to $N-1$. Menezes teaches prime integers (pg. 64, lines 2.92). It is commonly known in the art at the time of the invention that a variable can be defined to be a prime number, and/or an integer ranging between selected values. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including a prime integer and an integer between selected values in the permutation equation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to have a permutation equation which can have an adjusted solution set to allow for changes to occur to enhance security.

As per claim 13:

Iida and Pfab substantially teach the method of claim 3. Not explicitly disclosed is the permutation is defined by the relationship: $X = (XO + DIRECTION * PITCH * j)$ modulo N where $PITCH$ ranges from 0 to $N-1$, $DIRECTION$ is either 1 or -1, XO ranges from 0 to $N-1$, and j varies from 0 to $N-1$ and initializing j and X and transferring step includes the sub-step of repeating N times the steps of: reading a byte of the data element from the first memory, the

Art Unit: 2137

place value of the byte read being equal to the current index; writing in the second memory the byte that was read from the first memory; and incrementing j and varying X . Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need and completing a fundamental subroutine to read-transfer-and write data between memories. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including a permutation into the data transfer and to implement a subroutine to allow for the automated transfer of components of memory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements.

As per claim 16:

Iida and Pfab substantially teach the machine-readable medium of claim 14. Not explicitly disclosed is where the permutation is defined by the relationship: $X(XO + \text{DIRECTION} * \text{PITCH} * j) \text{ modulo } N$ where PITCH ranges from 0 to $N-1$, DIRECTION is either 1 or -1, XO ranges from 0 to $N-1$, and j varies from 0 to $N-1$. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including a permutation into the

Art Unit: 2137

data transfer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements.

As per claim 17:

Iida and Pfab substantially teach the machine-readable medium of claim 16. Not explicitly disclosed is the defining step, the value of PITCH is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2.1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 19:

Iida and Pfab substantially teach the machine-readable medium of claim 16. Not explicitly disclosed is in the defining step, the value of XO is chosen randomly before each transfer of the data element. Menezes teaches random variable, the defining of a random function, and the variability of the random variables (pg. 51, section 2,1.3). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including random variables in the permutation. This modification would have been obvious because a person having ordinary skill in the art would

Art Unit: 2137

have been motivated to do so, as suggested by Menezes, in order to expect that a random variable would be created to ensure that a permutation was randomly altered to enhance the security of the data transfer.

As per claim 20:

Iida and Pfab substantially teach the machine-readable medium of claim 16. Not explicitly disclosed is PITCH and N are mutually prime numbers. Menezes teaches mutually prime numbers, relatively prime, or co-prime if $\gcd(a,b) = 1$ (pg. 64, section 2.91). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including mutually prime numbers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to not have degenerate permutation functions, therefore enhancing the security of the data transfer.

As per claim 21:

Iida and Pfab substantially teach the machine-readable medium of claim 16. Not explicitly disclosed is where the permutation is defined by the relationship: $X = (XO + \text{DIRECTION} * \text{PITCH} * j) \text{ modulo } N$ where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, XO ranges from 0 to N-1, and j varies from 0 to N-1 and initializing j and X and transferring step includes the sub-step of repeating N times the steps of: reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index; writing in the second memory the byte that was read from the first memory; and incrementing j and varying X. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at

Art Unit: 2137

the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need and completing a fundamental subroutine to read-transfer-and write data between memories, Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including a permutation into the data transfer and to implement a subroutine to allow for the automated transfer of components of memory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements

As per claim 24:

Iida and Pfab substantially teach the programmable circuit of claim 22. Not explicitly disclosed is where the permutation is defined by the relationship: $X = (XO + \text{DIRECTION} * \text{PITCH} * j) \text{ modulo } N$ where PITCH ranges from 0 to N-1, DIRECTION is either 1 or, -1, XO ranges from 0 to N-1, and j varies from 0 to N-1. Menezes teaches permutations are functions, which are often used in various cryptographic constructs (PG. 10, section 1.3.2). It is commonly known in the art at the time of the invention was made to assume that a form of a permutation could be developed which would suite a desired application by anyone with a need. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system of Iida and Pfab by including a permutation into the data transfer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Menezes, in order to securely transfer the data elements.

Art Unit: 2137

**References Cited, Not Used*


The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US Patent No. 6,408,075 has been cited because it is relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Nadia Khoshnoodi
Examiner
Art Unit 2137
10/11/2006

NK


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER